REMARKS

After entry of the above amendments, claims 31-41 will be pending in the present application. Previously withdrawn claims 1-21 and 26-30 have been cancelled. Claims 22-25 have also been cancelled. New claims 31-41 have been added. Support for the new claims can be found in the specification, drawings, and claims as originally filed. No new matter has been added.

In this Amendment, Applicant has cancelled previously pending claims 1-30 from further consideration in this application. Applicant is not conceding that the subject matter encompassed by claims 1-30 is not patentable over art cited by the Examiner. Claims 1-30 have been cancelled in this Amendment solely to facilitate expeditious prosecution of the present application. Applicant reserves the right to pursue claims directed to the subject matter encompassed by claims 1-30 and any additional claims in one or more continuing and/or divisional applications.

Claim Objections

Previously pending claim 22 was objected to on the basis of informalities. Since claim 22 has been cancelled, Applicant respectfully requests withdrawal of the claim objection.

§ 102 Rejections

Previously pending claims 22-25 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 7,058,978 to Feuerstein et al. (hereinafter "Feuerstein").

New claim 31 recites:

31. A system comprising:
a network;
a satellite server connected to the network; and
a central server communicating with the satellite server via the network, the central server including
a master data storage storing master data,

a checker using a checking algorithm to generate a verification record for satellite data to be distributed to the satellite server, the satellite data being derived from the master data,

a distributor distributing the satellite data and the checking algorithm used to generate the verification record for the satellite data to the satellite server, and

a security monitor

monitoring for status messages from the satellite server,

responsive to receiving a status message from the satellite server during a scheduled time interval or in response to a status request sent to the satellite server, determining whether the satellite data at the satellite server is corrupted based on the received status message, and

responsive to not receiving a status message from the satellite server during a scheduled time interval or in response to a status request sent to the satellite server, determining that the satellite data at the satellite server is corrupted,

responsive to the security monitor determining that the satellite data at the satellite server is corrupted, the distributor re-distributing the satellite data to the satellite server.

In the Office action, the Examiner states:

> Feuerstein et al. discloses the one or more servers include a central server (file server 110; fig. 4) communicating with the substantially user inaccessible data storage (memory 430; fig. 4; col. 7, lines 45-50), said central server being protected by a firewall (network service provider 104; fig. 1); and a satellite server (front end network server 108; fig. 1) communicating with the user accessible data storage (memory 402; fig. 4), the satellite server (network server 108) being connected with the central server (file server 110; fig. 4) by a network (IP network 106; fig. 4).

(August 30, 2007 Office action, pg. 4).

The Examiner appears to be construing the "back-end file server 110" in Feuerstein as disclosing the "central server" recited in claim 31. Claim 31, however, recites that the "central server" includes "a checker using a checking algorithm to generate a verification record for satellite data to be distributed to the satellite server". In contrast, Feuerstein teaches that the "checksum value 428" is formulated by the "integrity verification component 418" located on the "front-end network server 108", which the Examiner has construed as disclosing the "satellite server" recited in claim 31.

Specifically, even though Feuerstein discusses the possibility of storing "checksum values" in the "back-end file server 110", Feuerstein never mentions locating "security component 414", which includes the "integrity verification component 418", on the "back-end file server 110". Thus, the generation of "checksum values" in Feuerstein does not occur on the "back-end file server 110".

Claim 31 also recites that the "central server" includes "a distributor distributing the satellite data and the checking algorithm used to generate the verification record for the satellite data to the satellite server". This is not taught by Feuerstein.

Additionally, claim 31 recites that the "central server" includes "a security monitor monitoring for status messages from the satellite server, responsive to receiving a status message from the satellite server during a scheduled time interval or in response to a status request sent to the satellite server, determining whether the satellite data at the satellite server is corrupted based on the received status message, and responsive to not receiving a status message from the satellite server during a scheduled time interval or in response to a status request sent to the satellite server, determining that the satellite data at the satellite server is corrupted".

In Feuerstein, everything in relation to verifying integrity of resources is handled by the "security component 414", which is located on the "front-end network server 108", not on the "back-end file server 110". In addition, Feuerstein does not disclose, teach, or suggest that the resource integrity verification process requires any sort of messaging between the "front-end network server 108" and the "back-end file server 110".

Further, in Feuerstein, verification of a resource's integrity only occurs when a request for the resource is received. In contrast, in claim 31, determination of whether "satellite data" is corrupted occurs at scheduled time intervals or in response to a request from the "central server". Feuerstein

does not disclose, teach, or suggest that resource integrity verification is scheduled or requested by the "back-end file server 110".

Hence, the "back-end file server 110" of Feuerstein cannot be construed as disclosing, teaching, or suggesting the "central server" recited in claim 31.

Accordingly, based at least on the reasons above, Applicant respectfully submits that claim 31, and the claims that depend therefrom, are not anticipated by Feuerstein.

CONCLUSION

On the basis of the above remarks, reconsideration and allowance of the claims is believed to be warranted and such action is respectfully requested. If the Examiner has any questions or comments, the Examiner is respectfully requested to contact the undersigned at the number listed below.

Respectfully submitted,
SAWYER LAW GROUP LLP

Dated: January 30, 2008

/Erin C. Ming/
Erin C. Ming
Attorney for Applicant
Reg. No. 47,797
(650) 475-1449